Министерство науки и высшего образования Российской Федерации федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

Факультет инфокоммуникационных технологий

**Основы кибербезопасности**

Практическая работа №6

**Выполнил**:

студент группы K34211

Швалов Даниил Андреевич

**Проверил**:

преподаватель практики, КТН

Назаров Михаил Сергеевич

Санкт-Петербург

2024

# Оглавление

[Введение 3](#__RefHeading___Toc6440_2741830133)

[Содержание отчета 4](#__RefHeading___Toc6442_2741830133)

[1. Описание системы 4](#__RefHeading___Toc8544_875968271)

[1.1. Назначение системы 4](#__RefHeading___Toc8544_875968271_Copy_2)

[1.2. Основной перечень ОТСС и ВТСС 5](#__RefHeading___Toc1518_4064630655)

[1.3. Циркулирующая информация 7](#__RefHeading___Toc6446_2741830133)

[2. Класс защищаемой системы 7](#__RefHeading___Toc8544_875968271_Copy_1)

[3. Определение необходимых систем защиты информации 8](#__RefHeading___Toc8544_875968271_Copy_1_)

[4. Системы защиты информации 9](#__RefHeading___Toc8544_875968271_Copy_11)

[4.1. Astra Linux Special Edition 9](#__RefHeading___Toc8544_875968271_Copy_12)

[4.2. Solar Next Generation Firewall 9](#__RefHeading___Toc8544_875968271_Copy_13)

[4.3. Solar Dozor 9](#__RefHeading___Toc8544_875968271_Copy_14)

[4.4. Solar appScreener 9](#__RefHeading___Toc8544_875968271_Copy_15)

[5. Конечная схема информационной системы 9](#__RefHeading___Toc8544_875968271_Copy_16)

[Вывод по работе 11](#__RefHeading___Toc7412_875968271)

# Введение

**Цель работы**. Изучить типовой алгоритм проектирования системы защиты информации в информационных системах. Приобрести практические навыки в классификации автоматизированных систем. Научиться подбирать средства защиты информации для защищаемых систем.

# Содержание отчета

## Описание системы

## Назначение системы

Информационным объектом для данной практической работы была выбрана коллегия адвокатов — негосударственная, независимая, самоуправляемая и самоконтролируемая организация профессиональных юристов, добровольно объединившихся в целях оказания квалифицированной юридической помощи физическим и юридическим лицам.

Коллегия адвокатов оказывает такие юридические услуги, как:

— проведение консультаций и составление справок по правовым вопросам;

— составление заявлений, жалоб и других документов правового характера;

— представление интересов в судопроизводстве;

— участие в качестве представителя доверителя.

Юридические услуги оказываются на основе гражданско-правового договора между адвокатом и доверителем.

Коллегия адвокатов обладает внутренней структурой, описанной в таблице 1.

Таблица 1 — Должности и обязанности в коллегии адвокатов

|  |  |
| --- | --- |
| **Должность** | **Обязанности** |
| Президент коллегии | Организация и планирование работы коллегии, заключение договоров и сделок, распоряжение средствами коллегии, осуществление контроля за работой адвокатов |
| Президиум коллегии | Руководство деятельности адвокатов и адвокатских консультаций, принятие и исключение из коллегии, поощрение адвокатов, организует проверки работы адвокатов |
| Совет коллегии | Организация и контроль за качеством работы адвокатов, разработка и принятие внутренних нормативных актов, управление финансами коллегии |
| Ревизионная комиссия | Ревизии финансово-хозяйственной деятельности коллегии |
| Технические специалисты | Разработка и поддержка информационно-технической инфраструктуры коллегии |

## Основной перечень ОТСС и ВТСС

На рисунке 1 приведена схема информационно-технической инфраструктуры рассматриваемой коллегии адвокатов.

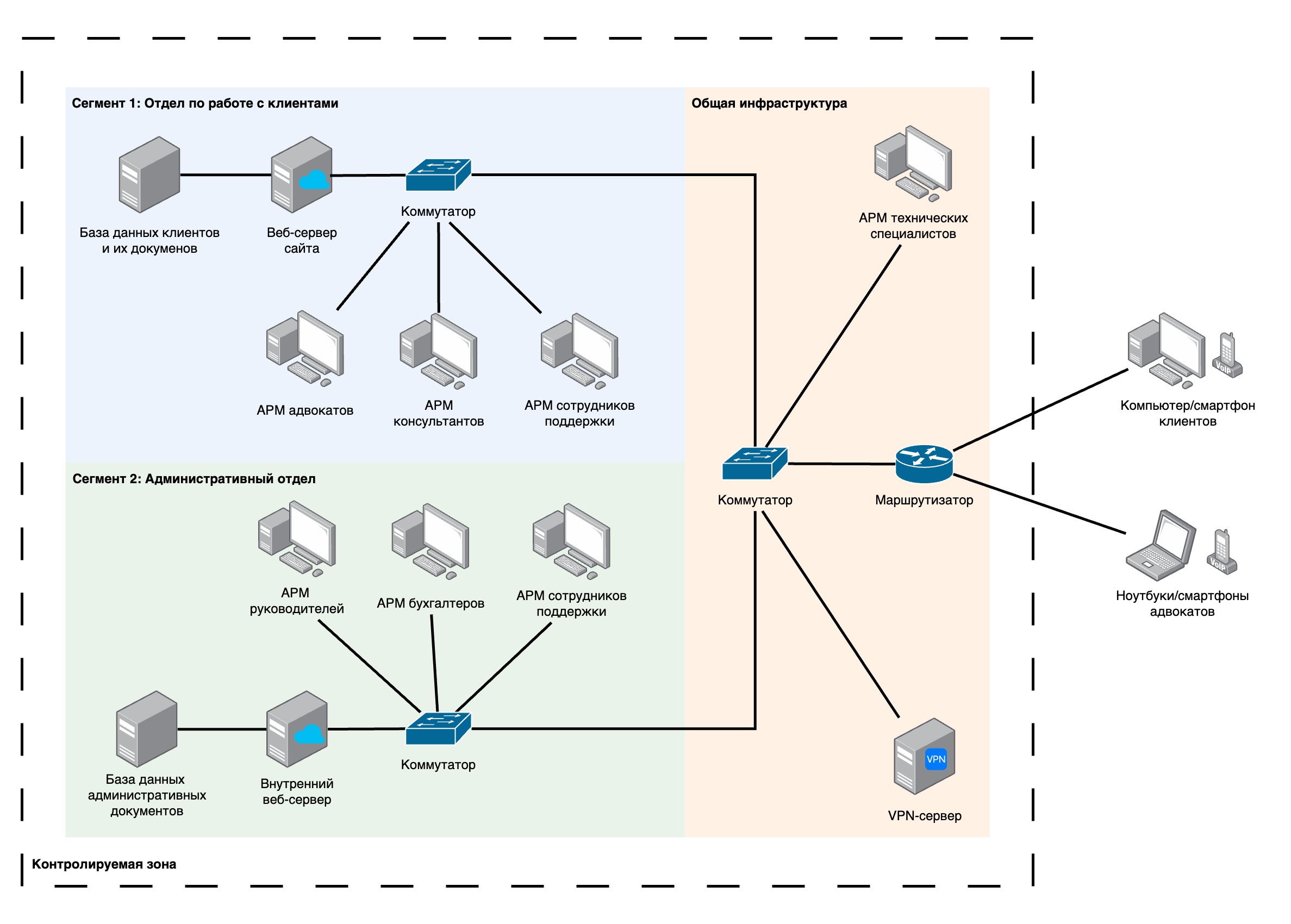


Рисунок 1 — Схема информационно-технической инфраструктуры коллегии адвокатов

Схема информационно-технической инфраструктуры, состоит из двух сегментов: отдела по работе с клиентами и отдела административного отдела. В совокупности, эти отделы состоят из следующих компонентов:

* веб-сервер, который обслуживает общедоступный информационный портал коллегии адвокатов и позволяет клиентам получить информацию или способ связи с коллегией;
* веб-сервер, который обслуживает внутренний информационный портал коллегии адвокатов, с которым работают сотрудники коллегии;
* VPN-сервер для безопасного доступа адвокатов в контролируемую зону;
* база данных клиентов, в которой хранятся данные, сохраняемые с веб-сервера (например, записи на прием, персональная информация, документы);
* база данных административных документов, где хранятся внутренние документы, связанные с работой коллегии;
* устройства для маршрутизации трафика;
* автоматизированные рабочие места и персональные устройства сотрудников;
* офисное оборудование (принтеры, сканеры и т. п.).

Предполагается, что клиенты могут иметь доступ только к информационному порталу коллегии адвокатов. Для взаимодействия с порталом предлагается использовать протокол HTTPS.

При этом самим адвокатам может понадобиться доступ к различным конфиденциальным документам. Для безопасной передачи данных предлагается использовать собственный VPN-сервер, например, на базе OpenVPN. Это позволит быть уверенным в том, что конфиденциальные данные передаются достаточно защищенно по сети.

Для настройки и поддержки информационно-технической инфраструктуры предлагается использовать автоматизированное рабочее место для технических специалистов, находящееся в контролируемой зоне.

## Циркулирующая информация

В коллегии адвокатов работают со следующими данными:

— информация о клиенте (ФИО, контактные данные, история обращений и т. п.);

— юридическая информация (документы, справки, выписки, судебное делопроизводство и т. п.);

— административная информация (информация об адвокатах, их ФИО, контактные данные, информация об их рабочей деятельности и т. п.).

Часть из перечисленных данных могут являться конфиденциальными, т. е. у злоумышленников или простых пользователей не должно быть прямого доступа к ним. Поэтому такие данные должны быть защищены должным образом.

## Класс защищаемой системы

Оба сегмента информационной системы являются многопользовательскими, т. е. в них одновременно обрабатывается и хранится информация разных уровней конфиденциальности, т. е. не все пользователи имеют право доступа ко всей информации.

Так, например, доступ к юридическим документам должен быть предоставлен только тем адвокатам, которые работают над соответствующим делом. Также, доступ к персональным данным сотрудников должен быть только у руководства и соответствующих сотрудников. У остальных сотрудников такого доступа быть не должно.

Исходя из этого, оба сегмента относятся к первой группе защищенности.

В первом сегменте «Отдел по работе с клиентами» предполагается хранить и обрабатывать различную информацию, связанную с клиентами. Примерами такой информации может выступать персональные данные, профессиональная или служебная тайна. При этом в ней не предполагается обрабатывать секретные данные. Таким образом, первый сегмент относится к классу 1Г.

Во втором сегменте «Административный отдел» предполагается хранить и обрабатывать информацию, связанную с работой коллегии. В качестве основных защищаемых данных будут выступать персональные данные сотрудников коллегии. В данном сегменте не предполагается обрабатывать ни служебную тайну, ни секретные данные. Исходя из этого, второй сегмент относится к классу 1Д.

Поскольку предполагается, что в системе будут работать несколько пользователей одновременно с разными уровнями доступа, то информационная система соответствует коллективному режиму обработки данных.

Таким образом, сегменты были отнесены к следующим классам:

* сегмент №1: класс 1Г;
* сегмент №2: класс 1Д.

Система в целом соответствует классу 1Г.

## Определение необходимых систем защиты информации

Для сегментов №1 и №2 с классами 1Г и 1Д соответственно актуальны подсистемы, представленные в таблице 2.

Таблица 2 — Подсистемы и требования для систем с классами 1Г и 1Д

|  |  |  |
| --- | --- | --- |
| **Подсистемы и требования** | **Классы** | |
| **1Г** | **1Д** |
| 1. Подсистема управления доступом |  |  |
| 1.1. Идентификация, проверка подлинности и контроль доступа субъектов: |  |  |
| в систему | + | + |
| к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ | - | + |
| к программам | - | + |
| к томам, каталогам, файлам, записям, полям записей | - | + |
| 1.2. Управление потоками информации | - | - |
| 2. Подсистема регистрации и учета |  |  |
| 2.1. Регистрация и учет: |  |  |
| входа (выхода) субъектов доступа в (из) систему (узел сети) | + | + |
| выдачи печатных (графических) выходных документов | - | + |
| запуска (завершения) программ и процессов (заданий, задач) | - | + |
| доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи | - | + |
| доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей | - | + |
| изменения полномочий субъектов доступа | - | - |
| создаваемых защищаемых объектов доступа | - | - |
| 2.2. Учет носителей информации | + | + |
| 2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей | - | + |
| 2.4. Сигнализация попыток нарушения защиты | - | - |
| 3. Криптографическая подсистема |  |  |
| 3.1. Шифрование конфиденциальной информации | - | - |
| 3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах | - | - |
| 3.3. Использование аттестованных (сертифицированных) криптографических средств | - | - |
| 4. Подсистема обеспечения целостности |  |  |
| 4.1. Обеспечение целостности программных средств и обрабатываемой информации | + | + |
| 4.2. Физическая охрана средств вычислительной техники и носителей информации | + | + |
| 4.3. Наличие администратора (службы) защиты информации в АС | - | - |
| 4.4. Периодическое тестирование СЗИ НСД | + | + |
| 4.5. Наличие средств восстановления СЗИ НСД | + | + |
| 4.6. Использование сертифицированных средств защиты | - | - |

## Системы защиты информации

Для проверки подлинности и контроля доступа субъектов, учета носителей информации и обеспечения целостности системы и хранимых данных были выбраны следующие системы защиты:

* Astra Linux Special Edition: для АРМ (в версии Desktop) и для веб-серверов (в версии Server).
* Solar Next Generation Firewall: для защиты внутренней сети от внешних атак;
* Solar Dozor: для контроля трафика и коммуникаций во внутренней сети, предотвращения утечек конфиденциальной информации;
* Solar appScreener: для поиска угроз и уязвимостей в используемом программном обеспечении.

Далее описаны основные сведения об этих системах защиты.

## Astra Linux Special Edition

Astra Linux Special Edition — сертифицированная операционная система со встроенными средствами защиты информаци для стабильной и безопасной работы ИТ-инфраструктур любого масштаба и обработки информации различной степени конфиденциальности. Она представлена в различных вариациях:

* Astra Linux Desktop для настольных компьютеров;
* Astra Linux Server для серверов;
* Astra Linux Mobile для планшетов и мобильных устройств;
* Astra Linux Embedded для встраиваемых систем.

Astra Linux обладает следующими преимуществами:

* поддержка различных процессорных архитектур;
* верифицированные средства защиты информации;
* совместимость с отечественным программным обеспечением;
* возможности для работы с гостайной, в том числе с грифом   
  «особой важности»;
* защищенные комплексы виртуализации;
* комплексы для обработки конфиденциальных сведений и персональной информации.

Astra Linux Special Edition внесен в Единый реестр отечественного ПО, сертифицирован ФСТЭК России и соответствует требованиям первого класса защиты операционных систем типа «А».

## Solar Next Generation Firewall

Solar Next Generation Firewall — это программный межсетевой экран, обеспечивающий комплексную защиту корпоративной сети от сетевых атак и вредоносного ПО, а также управление доступом к веб-ресурсам.

Solar Next Generation Firewall обладает следующим функционалом:

* предотвращение вторжений, защита от топ-200 актуальных атак с производительностью IPS до 20 Гбит/с;
* URL-фильтрация и фильтрация содержимого;
* SSL-инспекция содержимого трафика на наличие угроз;
* контроль сетевого трафика прикладных приложений.

Solar Next Generation Firewall внесен в Единый реестр отечественного ПО, сертифицирован ФСТЭК России и соответствует требованиям к межсетевым экранам по профилю защиты типа «А» и профилю защиты систем обнаружения вторжений уровня сети четвертого класса защиты.

## Solar Dozor

Solar Dozor — это высокопроизводительная система предотвращения утечек конфиденциальной информации, корпоративного мошенничества, профилактики и расследования инцидентов.

Solar Dozor обладает следующим функционалом:

* предотвращение утечек в реальном времени;
* полное покрытие всех каналов передачи данных;
* превентивное выявление нарушений с помощью поведенческого анализа;
* предупреждение инцидентов, связанных с внутренними нарушителями;
* инструменты для расследования инцидентов.

Solar Dozor внесен в Единый реестр отечественного ПО, сертифицирован ФСТЭК России и соответствует четвертому уровню контроля и технических условий.

## Solar appScreener

Solar appScreener — это система для обеспечения комплексной безопасность разработки приложений на основе технологий статического, динамического анализа, анализа состава и цепочки поставок ПО.

Solar appScreener обладает следующим функционалом:

* всесторонний контроль безопасности ПО основными видами анализа кода (SAST, DAST, OSA);
* анализ бинарного кода, проверка мобильных приложений по ссылке в App Store или Google Play и готовых веб-приложений;
* поддержка 36 языков программирования, 10 форматов исполняемых файлов и программ-полиглотов;
* формирование детального отчет с результатами разных видов анализа кода и списком найденных уязвимостей в коде.

## Конечная схема информационной системы

В соответствии с вышеперечисленными средствами защиты информации, схема, представленная на рисунке 1, была дополнена. Конечная схема информационной системы представлена на рисунке 2.

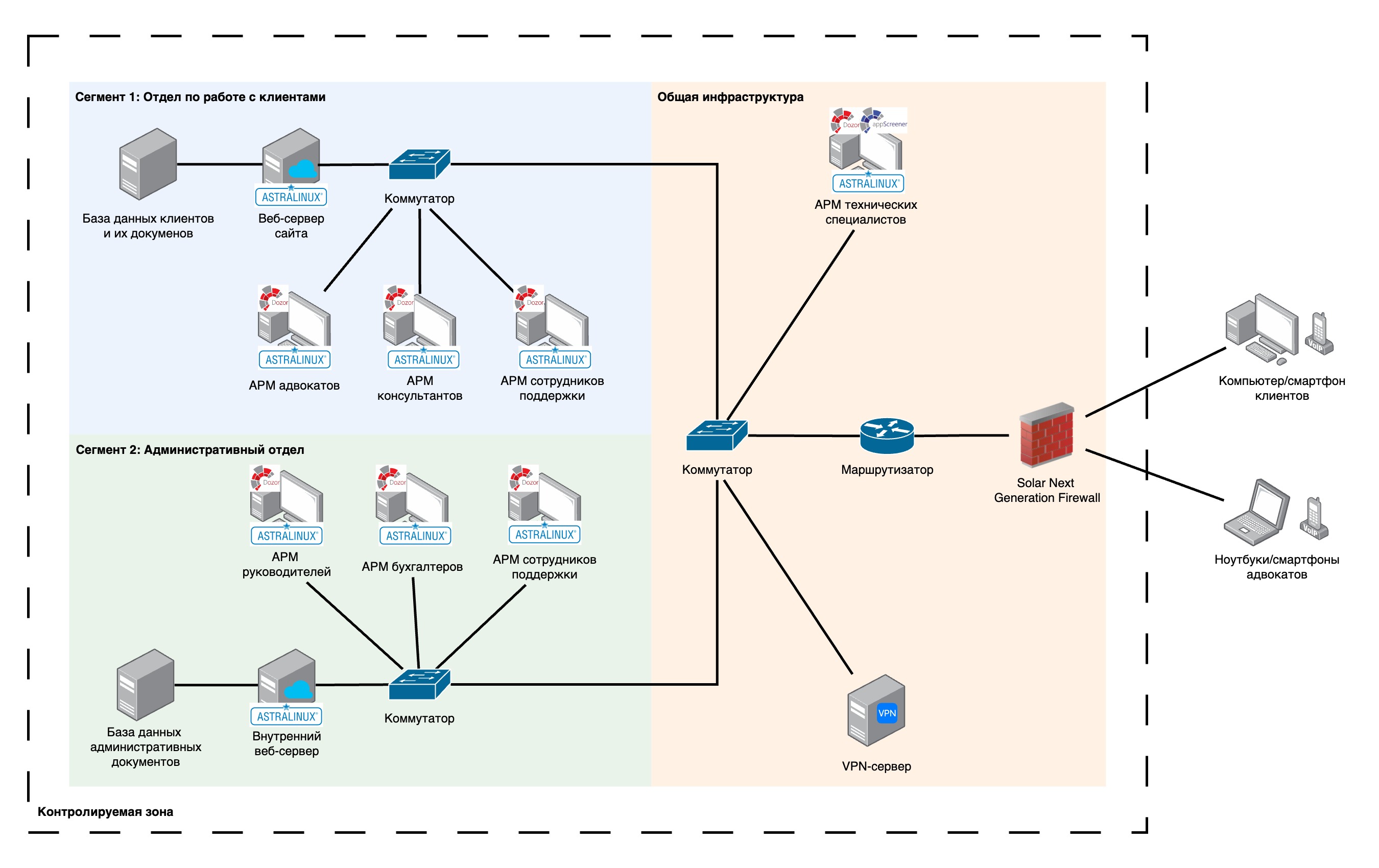


Рисунок 2 — Схема информационно-технической инфраструктуры коллегии адвокатов

# Вывод по работе

В результате выполнения данной практической работы был изучен типовой алгоритм проектирования системы защиты информации в информационных системах, приобретены практические навыки в классификации автоматизированных систем, получены навыки подбора средств защиты информации для защищаемых систем.